Notes for Algebraic Structures

Spring 2016

Transcribed by Jacob Van Buren
(`jvanbure@andrew.cmu.edu`)

Notes for Algebraic Structures, taught Spring 2016 at Carnegie Mellon University, by Professor Clinton Conley.

Administrativia

Instructor. Clinton Conley (`clintonc@andrew.cmu.edu`), WEH 7121
`http://www.math.cmu.edu/~clintonc/`

Grading. 20% HW, 20% $\times$ 2 midterms, 40% Final

Homework. Wednesday-Wednesday. Graded for completeness, one starred problem for which no collaboration of any type is allowed.
Most homework out of textbook ("D&F").

Contents

The Integers

Lecture 1 (2016–01–11)

Notation. $\mathbb{N} := \{1, 2, 3, \ldots\}$ in this class.

Properties: Order, other things. Least element in a set S: $x \in S$ s.t. $\forall y \in S, x \leq y$
Addition $(\mathbb{Z}, +)$:

- <u>Associativity</u> $(x + y) + z = x + (y + z)$
- <u>Identity</u> $x + 0 = 0 + x = 0$
- <u>Inversion</u> $x + (-x) = (-x) + x = 0$
- <u>Commutativity</u> $x + y = y + x$

Multiplication $(\mathbb{Z}, +, \cdot)$:

- <u>Associative</u>
- <u>Distributive</u>
- <u>Identity</u> ("1")

<u>Integer division</u>: Assume x an integer and $y \in \mathbb{Z}^+$ then $\exists! d \in \mathbb{Z}, \exists! r \in \mathbb{Z} : 0 \leq r < y, x = d \cdot y + r$

Definition 1. $y|x$ "y divides x" iff $\exists d \in \mathbb{Z} : x = d \cdot y$.

E.g. $3|9, 4 \not| 7$.

Definition 2. d is a <u>gcd</u> of x and y if

- $d|x, d|y$
- If $c|x$ and $c|y$ then $c|d$

Lecture 2 (2016–01–13)

Definition 3. Given $a, b \in \mathbb{Z}$, denote by $\mathbb{Z}(a, b)$ the set $\{ax + by | x, y \in \mathbb{Z}\}$.

Theorem 4 (Euclid, Bezout). *Suppose $a, b \in \mathbb{Z}$ are nonzero and let d be the smallest positive element of $\mathbb{Z}(a, b)$, then d is the unique positive GCD of a and b.*

Proof. d is a gcd of a, b

(1) (Existance of positive GCD)
   (a) By integer division, $\exists q \in \mathbb{Z}, \exists r \in \mathbb{Z}$ with $0 \leq r < d$ such that $a = qd + r$. If $r = 0$ then $d|a$, so done. Otherwise, suppose $0 < r < d$, so $r = a - qd$ since $d \in \mathbb{Z}(a, b)$, we may fix x, y st $d = ax + by$, meaning $r = a - q(ax + by) = a(1 - qx) + b(-qy)$, so $r \in \mathbb{Z}(a, b)$, meaning d was not the minimal positive element in $\mathbb{Z}(a, b)$, RAA. Thus, $d|a$
   (b) HW: If $c|a$ and $c|b$ then $c|(ax + by)$ for all $x, y \in \mathbb{Z}$ Hence $c|d$

(2) (Uniqueness of positive GCD) Suppose d_1, d_2 are both positive gcds of a and b. $d_1 | d_2$ and $d_2 | d_1$ as they are both gcds. i.e., $\exists m, n \in \mathbb{Z}$ such that $d_2 = md_1$ and $d_1 = nd_2$. As $\operatorname{sgn}(d_1) = \operatorname{sgn}(d_2)$, $m \geq 0$ and $n \geq 0$. As $d_1 = mnd_1$, $m = n = 1$. Thus $d_1 = d_2$. □

Definition 5. <u>Relatively prime</u> $\iff$ $\gcd(a, b) = 1$

Theorem 6. *Suppose p is prime and $a, b \in \mathbb{Z}$ are nonzero, and $p | (ab)$ then $p | a$ or $p | b$.*

Proof. Consider $d = \gcd(p, a)$. Since $d | p$, we know $d = p$ or $d = 1$.

If $d = p$: By def of GCD, $d | p$ and $d | a$ ie. $p | p$ and $p | a$ so we're done.
If $d = 1$: Fix integers x and y such that $px + ay = 1$. $b = p(xb) + (ab)y$ as $p | p(xb)$ and $p | \underbrace{(ab)}_{\uparrow} y$, $p | b$.

□

Theorem 7 (Unique Prime Factorization). *Suppose that $a > 1$ an integer, $m, n \geq 1$ and $p_1 \leq p_2 \leq \ldots \leq p_m, q_1 \leq q_2 \leq \ldots \leq q_m$ are positive primes.*

Then $m = n$ and $p_i = q_i$ for all i.

Proof. By induction, it suffices to show $p_1 = q_1$. Suppose not. WLOG, assume $p_1 < q_1$. We know that $p_1 | a$ (as $p_1 | q_1 q_2 \ldots q_n$) Hence, $\exists i \leq n$ such that $p_i | q_i$. since p_i and q_i prime, $p_1 = q_i$. However, $p_1 < q_1 \leq q_i = p_1$ so $p_1 < p_2$ contradiction.
Hence $p_1 = q_1$ so by induction, we're done. □

Lecture 3 (2016–01–15)

Teaser: Construct numbers of the form $a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$.
Notion of addition still exists: (similar to complex numbers, coefficients remain integers)
Same with multiplication
Among these "numbers", 2 is irreducible. But, 2 is not prime, as $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 + \sqrt{-5})$, but $2 | \underbrace{(1 + \sqrt{-5})(1 - \sqrt{-5})}_{=6=2\cdot 3}$.

The Integers (mod n)

For today, $n > 0$.

Definition 8. For $a, b \in \mathbb{Z}$ we say $a \equiv b \pmod{n}$ iff $n \,|\, (b - a)$.

$\equiv$ is an *equivalence relation*

- Reflexivity: $a \equiv a$
- Symmetry: $a \equiv b \iff b \equiv a$
- Transitivity: $a \equiv b \wedge b \equiv c \implies a \equiv c$

Proof. We know that $a \equiv b$ and $b \equiv c$, i.e. $n \,|\, (b - a)$ and $n \,|\, (c - b)$ We want $a \equiv c$, i.e., $n \,|\, (c - a)$

$$c - a = c + (-b + b) - a = \underbrace{(c - b) + (b - a)}_{n \text{ divides these}}$$

$\square$

Definition 9. Denote by $\overline{a}$ or $[a]_n$ the <u>equivalence class</u> of a with respect to $\equiv \pmod{n}$ (I.e., The set $\{b \in \mathbb{Z} : a \equiv b \pmod{n}\} = \overline{\{a + kn : k \in \mathbb{Z}\}}$).

Example. If $n = 2$, there are 2 equivalence classes:
$\overline{0} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \overline{2} = \overline{-36}$
$\overline{1} = \{\ldots, -3, -1, 1, 3, \ldots\}$

Definition 10. Denote by $\mathbb{Z}/n\mathbb{Z}$ the collection of all $\equiv \pmod{n}$ equivalence classes.

E.g. $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$
"Define" addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ as follows:

$$\overline{a} + \overline{b} = \overline{a + b}$$
$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Makes sense, but we need to check that this definition makes any sense at all (make sure it's *well-defined*). Specifically, we need to make sure that the results of these operations doesn't depend on the representatives of the equivalence classes we chose (e.g. check that $\overline{x} + \overline{z} \equiv \overline{y} + \overline{z}$ if $x \equiv y$).
For brevity, we just show addition.

Theorem 11. *$+$ and $\cdot$ are well-defined on $\mathbb{Z}/n\mathbb{Z}$*

Proof. (of $\cdot$) Assume that $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Then, we want to show that $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.
We know: $n \,|\, (a_2 - a_1)$ and $n \,|\, (b_2 - b_1)$.

We want: $n\,|\,(a_2b_2 - a_1b_1)$.

$$\begin{aligned} a_2b_2 - a_1b_1 &= a_2b_2 + (-a_1b_2 + a_1b_2) - a_1b_1 \\ &= (a_2b_2 - a_1b_2) + (a_1b_2 - a_1b_1) \\ &= \underbrace{(a_2 - a_1)b_2 + a_1(b_2 - b_1)}_{n \text{ divides these}} \end{aligned}$$

So, $n\,|\,(a_2b_2 - a_1b_1)$ as desired $\square$

Remark: This is a special case of a "quotient construction," in which you start with a set and an equivalence relation on it and operations on the set that "respect" the equivalence relations (i.e. equivalent inputs yield equivalent outputs)
Moar notes: Mutiplicative inverses are uncommon in the integers (only for 1 and -1). However, it's "more prevalent" in $\mathbb{Z}/n\mathbb{Z}$ in the following sense:

THEOREM 12. *Suppose* $n > 0$ *is an integer,* $a \in \mathbb{Z}$ *such that* $\gcd(n, a) = 1$ *(they're coprime). Then there is* $b \in \mathbb{Z}$ *such that* $ab = 1 \pmod{n}$ *(alternatively,* $\overline{a} \cdot \overline{b} = \overline{1}$*)*

PROOF. Use Bezout's theorem (from last lecture) Take integers x, y such that $nx + ay = \gcd(a, n) = 1$. Then, $nx = 1 - ay$, so $n\,|\,(1 - ay)$, so $1 \equiv ay \pmod{n}$, Choose $b = y$ and we're done ($\overline{a}\overline{b} \equiv \overline{1}$). $\square$

Groups

DEFINITION 13. We say that $*$ is a binary operation on some set X if it is a function $* : X \times X \to X$. (That is, $*$ accepts two (ordered) inputs from X and it outputs one element of X.)

Remark: usually write $a * b$ for the output of $*$ on the input (a, b).

DEFINITION 14. A group is a set G with a binary operation $*$ (often abbreviated $(G, *)$) satisfying the following 3 axioms.

i. Associativity: $\forall a, b, c \in G : (a * b) * c = a * (b * c)$
ii. Identity: There is some $e \in G$ such that $\forall a \in G : a * e = e * a = a$
iii. Inversion: $\forall a \in G(\exists b \in G(a * b = b * a = e))$ (where e is as described in ii)

Index